**WHAT IS CLAIMED IS:**

1. A method for preventing malicious network attacks said method comprising:
receiving a packet from a client computer;
determining a number of packets received during a time interval; and
rejecting the packet in response to the number of packets exceeding a packet limit.

2. The method as described in claim 1 wherein the client computer is identified by a source IP address.

3. The method as described in claim 1 wherein the determining further includes:
identifying a client data area based on a source IP address, the client data area including the number of packets received; and
incrementing the number of packets received.

4. The method described in claim 1 further comprising:
determining an action from a plurality of actions based on the number of packets received; and
executing the action.

5. The method described in claim 1 further comprising:
receiving a socket request from the client computer;
determining a number of sockets opened for the client computer;
comparing the number of sockets opened to a socket limit; and
determining whether to allow a socket request based on the comparison.

6. The method described in claim 1 further comprising:
creating configuration settings, the configuration settings including the packet limit.

7. The method described in claim 6 further comprising:
providing a test script, the test script including one or more attack simulations;
processing the attack simulations included in the test script;
determining whether to change the configuration settings based on the processing; and
changing the configuration settings based on the determination.

8. An information handling system comprising:
one or more processors;
a memory accessible by the processors;
one or more nonvolatile storage devices accessible by the processors;
a network interface for receiving packets from a computer network; and
an packet handling tool to manage packets received from the network interface, the packet handling tool including:
means for receiving a packet from a client computer through the network interface;
means for determining a number of packets received during a time interval; and
means for rejecting the packet in response to the number of packets exceeding a packet limit.

9. The information handling system as described in claim 8 further comprising:
means for identifying the client computer by a source IP address.

10. The information handling system as described in claim 8 wherein the means for determining further includes:
means for identifying a client data area based on a source IP address, the client data area including the number of packets received; and
means for incrementing the number of packets received.

11. The information handling system as described in claim 8 further comprising:
means for receiving a socket request from the client computer;
means for determining a number of sockets opened for the client computer;
means for comparing the number of sockets opened to a socket limit; and
means for determining whether to allow a socket request based on the comparison.

12. The information handling system as described in claim 8 further comprising:
means for creating configuration settings, the configuration settings including the packet limit.

13. The information handling system as described in claim 12 further comprising:
means for providing a test script, the test script including one or more attack simulations;

means for processing the attack simulations included in the test script;

means for determining whether to change the configuration settings based on the processing; and

means for changing the configuration settings based on the determination.

14. A computer program product for preventing malicious network attacks, said computer program product comprising:

means for receiving a packet from a client computer;

means for detecting a number of packets received during a time interval; and

means for rejecting the packet in response to detecting that the number of packets exceeds a packet limit.

15. The computer program product as described in claim 14 wherein the client computer is identified by a source IP address.

16. The computer program product as described in claim 14 wherein the determining further includes:

means for identifying a client data area based on a source IP address, the client data area including the number of packets received; and

means for incrementing the number of packets received.

17. The computer program product described in claim 14 further comprising:

means for determining an action from a plurality of actions based on the number of packets received; and

means for executing the action.

18. The computer program product described in claim 14 further comprising:

means for receiving a socket request from the client computer;

means for determining a number of sockets opened for the client computer;

means for comparing the number of sockets opened to a socket limit; and

means for determining whether to allow a socket request based on the comparison.

19. The computer program product described in claim 14 further comprising:

means for creating configuration settings, the configuration settings including the packet limit.

20. The computer program product described in claim 19 further comprising:

means for providing a test script, the test script including one or more attack simulations;

means for processing the attack simulations included in the test script;

means for determining whether to change the configuration settings based on the processing; and

means for changing the configuration settings based on the determination.